



CNA e-Tool HUD User Access Guide

U.S. Department of Housing and Urban Development (HUD)

Federal Housing Administration (FHA)

August 2017



Document History

Version No.	Date	Author	Revision Description
1.0	08/17/2017	Sean Cortopassi	Final



Contents

1.	Getting Started	3
1.1	Intended Audience	3
2.	HUD Employee Access	3
2.1	HUD Employee Authentication	3
2.2	HUD Employee Authorization	4
2.3	HUD Employees Accessing the CNA e-Tool from Secure Systems	4
2.4	HUD Employees Secure Systems Help Desk Support	6
2.5	HUD Employees HITS & DIAMS Help Desk Support	7
3.	Note about Personally Identifiable Information	7
4.	Note about sharing passwords and credentials	7
	Appendix A: CNA E-TOOL RULES OF BEHAVIOR	8

1. Getting Started

The Capital Needs Assessment (CNA) e-Tool automates the process for the preparation, submission and review of a CNA. The CNA e-Tool home web page can be found at the following link:

https://portal.hud.gov/hudportal/HUD?src=/program_offices/housing/mfh/cna

The CNA e-Tool is an application that is hosted on the Secure Systems Platform. Obtaining access to any secure system application is a two-step process consisting of authentication and authorization.

User Authentication is a process of verifying user credentials on a system level to ensure that the user has access to the system in general. HUD User credentials are typically provided in a form of a username or user ID and a password, and are checked against the enterprise-level database Active Directory (AD).

User Authorization is done on an application level to determine what application(s) and its function(s) the user is authorized to access. Authorization rights are typically set up by assigning application-specific roles and/or actions to the user ID inside the application database and are checked by the application process.

1.1 Intended Audience

This document is intended to serve as a user access guide for HUD employees on CNA e-Tool authentication and authorization.

The following ID credentials that are available are as follows:

❖ **HUD Federal Employees:** HUD ID (H ID)

❖ **HUD Contractor Employees:** Contractor ID (C ID)

2. HUD Employee Access

All HUD employees will access the CNA e-Tool application with their H ID or C ID through the Secure Systems website on the HUD intranet at the following link: <https://hudapps.hud.gov/ssmaster>. H ID and C ID users can access the URL link above from the HUD intranet.

2.1 HUD Employee Authentication

H ID and C ID and passwords are the authentication credentials for HUD federal employees and contractor employees.

2.2 HUD Employee Authorization

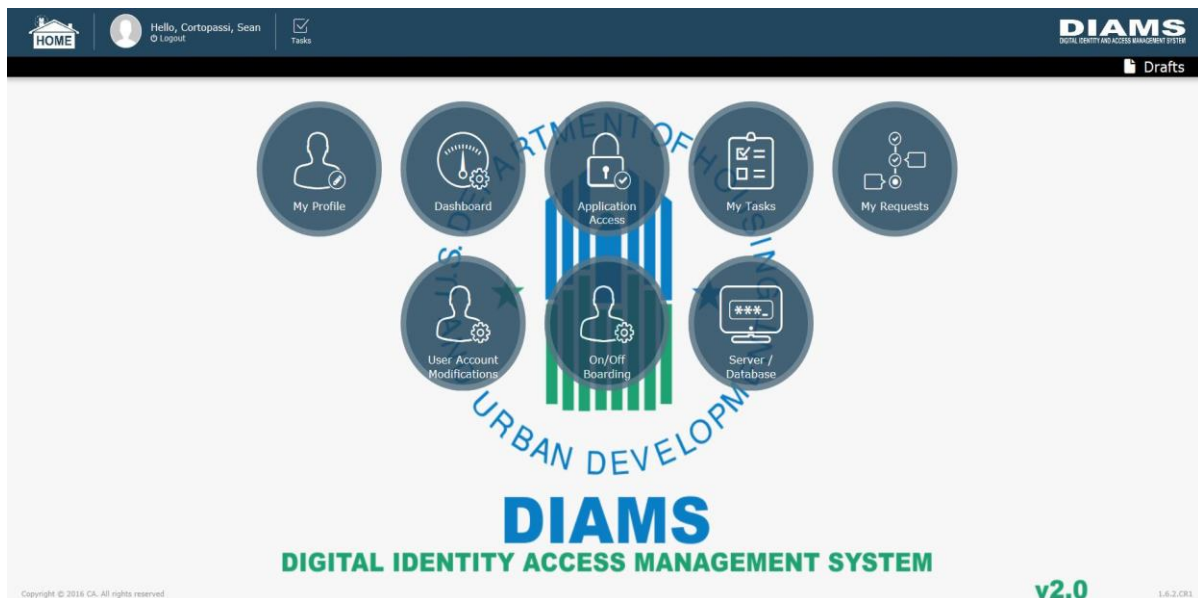
1. The H ID User who requires access should send an email to their supervisor and request that they submit a Digital Identity Access Management System (DIAMS) request on their behalf for the CNA E-TOOL - P282.

The C ID User should send an email to their Government Technical Monitor (GTM) and request that they submit a DIAMS request on their behalf for the CNA E-TOOL - P282.

(Note: The requester's supervisor/GTM must also request that the DIAMS request include Secure Systems- P104 if the requesting H ID User or C ID User does not already have Secure Systems access).

2. The requesting H ID User's supervisor or C ID User's GTM will submit the request using DIAMS. The request will be saved within HUD's Information Technology Service (HITS) National Help Desk System where it will be routed to the designated approving official. The approving official is responsible for approving access to the application request. If the approval is not approved within two weeks, then send an email to CNAaccess@hud.gov to let the System Administrator know.
3. The H ID User or C ID User and their requesting supervisor/GTM will receive an email once the approving official has taken an action on a request for application access.

DIAMS is located at <http://diams.hud.gov/sigma/app/index#/home>




Note: HUD Federal and Contractor Employees must be authorized users of Secure Systems before they can use the CNA e-Tool Application. Secure Systems access requests can be submitted while requests for the CNA e-Tool are requested in DIAMS.

2.3 HUD Employees Accessing the CNA e-Tool from Secure Systems

After Secure Systems access and CNA roles have been granted, HUD federal and contractor employees will be able to login to Secure Systems at the following link: <https://hudapps.hud.gov/ssmaster/>.

After pressing the link above the user will be redirected to the following page that needs to be reviewed in detail.

Note: Secure Systems has setup single sign-on for the HUD employee based on their AD information. However, in some circumstance the user will need to login with their H ID or C ID and LAN Password.


Secure Systems

User Login
[faq](#) | [help](#) | [search](#) | [home](#) | [logout](#)

You must login at least once every 90 days to maintain an active ID. If you do not login again before 2 Mar 2017, your ID will be automatically deactivated. If your User ID is deactivated, please contact the TAC to reactivate your ID.

Legal Warning

Misuse of Federal Information through the HUD Secure Connection web site falls under the provisions of title 18, United States Code, Section 1030. This law specifies penalties for exceeding authorized access, alterations, damage, or destruction of information residing on Federal Computers.

Warning Notice

The Secure Systems security access software supports Internet Explorer 7.0 browser. Other browsers may not be compatible with this software.

Message of the Day

**** Attention All Users ****


The following **Multifamily** applications will be down between **8:00pm EST Friday December 16th** until **12:00pm EST Saturday December 17th** for Maintenance.

APPS, M2M, MDDR, TRACS/ARAMS, IREMS

We apologize for any inconvenience.

(Message ID# 1400 - Updated by C00722 on Tue Dec 06 08:03:38 EST 2016)

After clicking the Accept button, the user will be redirected to the Secure Systems Main Menu which will list links to all applications that the user ID has been authorized to access. The user must select the CNA e-Tool Application.


Secure Systems

Main Menu
[faq](#) | [help](#) | [search](#) | [home](#) | [logout](#)

Welcome WILLIAM ANDERSON

system administration

- BPR Authorization Letter History Report
- Business Partners Maintenance
- Extra Coordinators Report
- PHA Assignment Maintenance
- Property Assignment Maintenance
- RAP Organization Assignment Maintenance
- TAC Report
- User Maintenance

systems

- CNA eTool**
- Enterprise Income Verification (EIV)
- Financial Assessment Submission - PHA (FASPHA)
- Grants Interface Management System (GIMS II)
- Mark-to-Market (M2M)
- Multifamily Delinquency and Default Reporting System (MDDR)
- Public Housing Assessment System: Scores and Status (NASS)
- Physical Assessment Subsystem (PASS)
- PIH Information Center (PIC)
- Test Site for PIH Information Center - PIC Test (PICTST)
- Quality Assurance Subsystem (QASS)
- Integrated Real Estate Management System (IREMS)

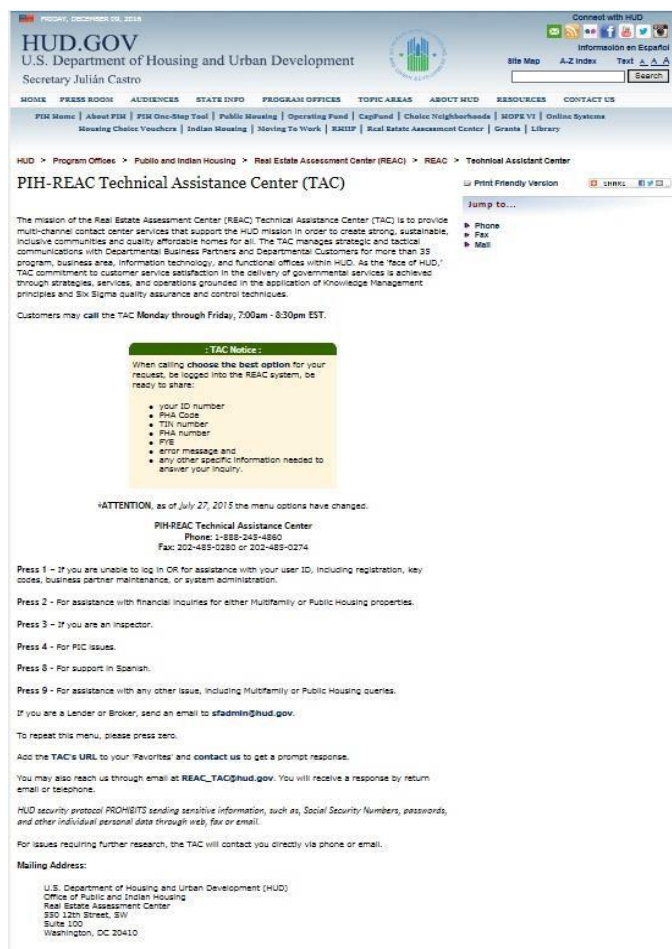
System Administration

- BPR Authorization Letter History Report
- Business Partners Maintenance


2.4 HUD Employees Secure Systems Help Desk Support

Help desk support for H ID and C ID users' application, authorization, and authentication questions for Secure Systems are provided by The Public and Indian Housing (PIH), The Real Estate Assessment Center (REAC), and The Technical Assistance Center (TAC). The help desk can be reached by phone at 1-888-245-4860 and is open Monday through Friday, 7:00am - 8:30pm EST. H ID and C ID's become inactive (requiring reactivation) after 90 days of inactivity (without logging into Secure System). In addition, REAC-TAC can be reached at the public website located at:

http://portal.hud.gov/hudportal/HUD?src=/program_offices/public_indian_housing/reac/support/tac



HUD.GOV
U.S. Department of Housing and Urban Development
Secretary Julián Castro


Connect with HUD
Information en Español
Site Map A-Z Index Text 

WOMEN PRESS ROOM AUDIENCES STATE INFO PROGRAM OFFICES TOPIC AREAS ABOUT HUD RESOURCES CONTACT US

PIH Home | About PIH | PIH One-Stop Tool | Public Housing | Operating Fund | CapFund | Choice Neighborhoods | WOPF VI | Online Systems
Rental Choice Vouchers | Indian Housing | Moving To Work | RRIIP | Real Estate Assessment Center | Grants | Library

HUD > Program Offices > Public and Indian Housing > Real Estate Assessment Center (REAC) > REAC > Technical Assistance Center

PIH-REAC Technical Assistance Center (TAC)

Print Friendly Version  Jump to...

Phone
Fax
Mail

The mission of the Real Estate Assessment Center (REAC) Technical Assistance Center (TAC) is to provide multi-channel contact center services that support the HUD mission in order to create strong, sustainable, inclusive communities and quality affordable homes for all. The TAC manages strategic and tactical communications with Departmental Business Partners and Departmental Customers for more than 35 program, business area, information technology, and functional offices within HUD. As the face of HUD, TAC commitment to customer service satisfaction in the delivery of governmental services is achieved through strategies, services, and operations grounded in the application of Knowledge Management principles and Six Sigma quality assurance and control techniques.

Customers may call the TAC Monday through Friday, 7:00am - 8:30pm EST.

TAC Notice:
When calling choose the best option for your request, be logged into the REAC system, be ready to share:

- your ID number
- PHA Code
- TTH number
- PHA number
- PVE
- error message and
- any other specific information needed to answer your inquiry.

ATTENTION: as of July 27, 2015 the menu options have changed:

PIH-REAC Technical Assistance Center
Phone: 1-888-245-4860
Fax: 202-485-0250 or 202-485-0274

Press 1 - If you are unable to log in OR for assistance with your user ID, including registration, key codes, business partner maintenance, or system administration.

Press 2 - For assistance with financial inquiries for either Multifamily or Public Housing properties.

Press 3 - If you are an Inspector.

Press 4 - For PIC issues.

Press 5 - For support in Spanish.

Press 9 - For assistance with any other issue, including Multifamily or Public Housing queries.

If you are a Lender or Broker, send an email to stadmin@hud.gov.

To repeat this menu, please press zero.

Add the TAC's URL to your 'Favorites' and contact us to get a prompt response.

You may also reach us through email at REAC_TAC@hud.gov. You will receive a response by return email or telephone.

HUD security protocol PROHIBITS sending sensitive information, such as, Social Security Numbers, passwords, and other individual personal data through web, fax or email.

For issues requiring further research, the TAC will contact you directly via phone or email.

Mailing Address:
U.S. Department of Housing and Urban Development (HUD)
Office of Public and Indian Housing
Real Estate Assessment Center
530 12th Street, NW
Suite 100
Washington, DC 20410

If an H ID became inactive, the H ID user should open a ticket with REAC-TAC. This process should take no more than 24 business hours to resolve. If your account is not unfrozen within two weeks, then send an email to CNAaccess@hud.gov to let the System Administrator know.

C ID users will need to have their GTM contact REAC-TAC on the contractor's behalf. It is possible that this may require a resubmission request using DIAMS.

When contacting the REAC-TAC help desk for User ID reactivation, users will be asked to verify their Secure System information, which includes: User ID, Mother's Maiden Name, and the last four digits of



their Social Security Number. Terminated user ID's can be reactivated by contacting the REAC-TAC help desk by phone at 1-888-245-4860.

2.5 HUD Employees HITS & DIAMS Help Desk Support

Help desk support for H ID and C ID users' who are having issues with their Local Area Network (LAN) Password or with their DIAMS request can contact the HITS National Help Desk at 888-297-8689.

3. Note about Personally Identifiable Information

During the registration and password reset processes you may be required to provide your Social Security Number (SSN) and your mother's maiden name to complete the registration and/or password reset processes. You may have concerns about providing that information and are wondering why may require sensitive personally identifiable information (PII).

According to government regulations, your SSN is required when trying to access a Federal computer system. HUD requires your SSN and mother's maiden name to verify your identity before processing the registration or password reset forms to issue you an ID or reset your password. The information is being entered into a secure environment and will be used exclusively for the registration or password reset processes.

Your SSN and mother's Maiden Name is considered PII. Your PII is protected by the Privacy Act of 1974, as amended (5 U.S. Code 552a). This information will only be used by Federal staff who hold positions of trust and who are specifically authorized to process your ID credentials or reset your password.

4. Note about sharing passwords and credentials

Users should never share their password or credential information with anyone. This would be a violation of government regulations, and it increases the number of threats to HUD, Secure Systems, the LAN, and could potentially jeopardize your PII. If it is determined that misuse with your access credential has occurred there will be penalties and future access/credentials will be revoked. More information is provided within the Rules of Behavior, which we ask that you please sign and email to CNAaccess@hud.gov after you receive your credential.

Appendix A: CNA E-TOOL RULES OF BEHAVIOR

CNA E-TOOL RULES OF BEHAVIOR

SECTION I - RESPONSIBILITIES

This section describes what ROB are, why they are needed, what users can expect, and the consequences for violating the ROB.

What are Rules of Behavior?

Office of Management and Budget (OMB) Circular A-130 Appendix III requires every System Security Plan (SSP) to contain a Rules of Behavior (ROB). ROB apply to the system users and list specific responsibilities and expected behavior of all individuals with access to or use of the named information system. In addition, ROB outlines the consequences of non-compliance and/or violations.

Why are Rules of Behavior Needed?

ROB is part of a complete program to provide good information security and raise security awareness. ROB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

Who is Covered by the Rules of Behavior?

The ROB covers all government and non-government users of the named information systems. This includes contract personnel and other federally funded users.

What are the Consequences for Violating the Rules of Behavior?

Penalties for non-compliance may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, reassignment, termination, and possible criminal and/or civil prosecution.

SECTION II - APPLICATION AND ORGANIZATION RULES

This section identifies the Rules of Behavior measures that will apply to Capital Needs Assessment Electronic Tool end-users. Section 3.1 lists the most common and minimal set of ROB as recommended by NIST 800-18. Section 3.2 lists other ROB that may apply to your organization. Section 2h includes ROB for system administrators. Each section is discussed in detail below.

A. Passwords

1. Passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as *#\$ %). Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.
3. Passwords must be unique to each user and must never be shared by that user with other users. For example, colleagues sharing office space must never share each other's password to gain system access.
4. Users who require multiple passwords should never be allowed to use the same password for multiple applications.
5. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as a Government Services Administration Security Container. If they are stored on a computer, this computer should not be connected to a network or the Internet. The file should be encrypted.

B. Encryption

1. Extremely sensitive data should be encrypted prior to transmission.
2. The sensitivity of the information needing protection, among other considerations, determines the sophistication of the encryption technology. In most circumstances, only the most sensitive or compartmentalized information should be encrypted.
3. Files that contain passwords, proprietary, personnel, or business information, and financial data typically require encryption before transmission, and should be encrypted while stored on the computer's hard disk drive.
4. Sensitive information that travels over wireless networks and devices should be encrypted.

*C. Internet Usage*

1. Downloading files, programs, templates, images, and messages, except those explicitly authorized and approved by the system administrator, is prohibited.
2. Visiting websites including, but not limited to, those that promote, display, discuss, share, or distribute hateful, racist, pornographic, explicit, or illegal activity is strictly prohibited.
3. Because they pose a potential security risk, the use of Web based instant messaging or communication software or devices are prohibited.
4. Using the Internet to make non-work related purchases or acquisitions is prohibited.
5. Using the Internet to manage, run, supervise, or conduct personal business enterprises is prohibited.

D. Email

1. Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited.
2. E-mail addresses and e-mail list-serves constitute sensitive information and are never to be sold, shared, disseminated, or used in any unofficial manner.
3. Using an official e-mail address to subscribe to any non-work related electronically distributed newsletter or magazine is prohibited.

E. Working from Home/Remote Dial-up Access

All CNA E-TOOL users are responsible for attending annual IT Security certification training. Failure to attend will result in having system access privileges revoked.

1. Users may dial into the network remotely only if pre-approved by the system administrator.
2. Users must be certain to log-off and secure all connections/ports upon completion.
3. Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. At no time should a "live" dial-up connection be left unattended.
4. Web browsers must be configured to limit vulnerability to an intrusion and increase security.
5. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable-modem) must install a hardware or software firewall.
6. No official material may be stored on the user's personal computer. All data must be stored on a floppy disk and then secured in a locked filing cabinet, locker, etc.
7. Operating system configurations should be selected to increase security.

F. Unofficial Use of Government Equipment

Except for limited personal use, government equipment including, but not limited to, fax machines, copying machines, postage machines, telephones, and computers are for official use only.

G. Other Rules of Behavior

To properly safeguard the Department's information assets while using information technology, it is essential for all employees to be aware of procedures for destroying sensitive information. Sensitive information within HUD that must be protected includes, but is not limited to, financial management information (budgeting, accounting, etc.); investigative information; contract sensitive information (pre-solicitation procurement documents, statements of work, etc.); and security management information (i.e., identification of systems security controls and vulnerabilities).

Of particular concern is Personally Identifiable Information (PII), which includes social security numbers, names, dates of birth, places of birth, parents' names, credit card numbers, applications for entitlements, and information relating to a person's private financial, income, employment, tax records, etc.

To assist you in determining what type of information should be considered sensitive, here are a few examples:

1. Personnel data
2. Travel vouchers
3. Procurement documents
4. Statements of Work or related procurement documents
5. Loan applications or files
6. Grant applications or files
7. COOP data



The May 25, 2006 memorandum from the Deputy Secretary and the June 6, 2006 broadcast email from the CIO to all HUD employees stated "Protect all electronic/optical media and hard copy documentation containing sensitive information and properly dispose of it by shredding hard copy documentation, or by contacting the HITS Help Desk to dispose of electronic/optical media".

In each Regional Office a location will be set up, in the Information Technology Division, where media containing sensitive data will be destroyed.

Please use the following procedures to properly destroy sensitive data stored on electronic/optical media that are no longer in need of maintaining:

1. Contact your supporting IT staff if you need media destroyed that contains sensitive information (CDs, DVDs, flash drives, Personal Verification Cards (PVC), external hard drives, etc.) and you will be provided with instructions.

In addition, absolutely no media containing sensitive information will be sent through the mail or released from the Department.

1. Using system resources to copy, distribute, utilize, or install unauthorized copyrighted material is prohibited.
2. Users who no longer require IT system access (as a result of job change, job transfer, or reassignment of job responsibilities) must notify the system administrator.
3. When not in use, workstations must be physically secured. Users must also log-off or turn-off the system.
4. Screen-savers must be password protected.
5. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
6. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person's account is prohibited.
7. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the system administrator.

H. Additional Rules of Behavior for CNA e-TOOL System Administrators

CNA e-TOOL system administrators have a unique responsibility above and beyond that of regular users. In addition to being regular system users, they also have special access privileges that regular users do not have. Therefore, they need to be susceptible to additional Rules of Behavior over and above the common user.

1. CNA e-TOOL System administrators may only access or view user accounts with the expressed consent of the user and/or management.
2. CNA e-TOOL System administrators may not track or audit user accounts without the expressed consent of the user and/or management.
3. CNA e-TOOL System administrators must make every reasonable effort to keep the network free from viruses, worms, Trojans, and unauthorized penetrations.
4. It is the CNA e-TOOL system administrators' responsibility to account for all system hardware and software loaned to system users for the execution of their official duties.
5. CNA e-TOOL system administrators are responsible for attending annual IT Security certification training. Failure to attend will result in having system access privileges revoked.

**SECTION III - ACKNOWLEDGMENT**

Prior to receiving authorization for CNA E-TOOL system access, every user should read and sign the ROB (this applies to system administrators since they are also "users" of the system). By signing the signature page, the user agrees to abide by the ROB and understands that failure to do so might be grounds for disciplinary action. Please retain a signed copy of the ROB for your personal records and submit the original signed copy to the CNA E-TOOL System Administrator for your local office.

I have read and understand the Rules of Behavior (ROB) governing my use of the Capital Needs Assessment Electronic Tool (CNA E-TOOL) and agree to abide by them. I understand that failure to do so may result in disciplinary action being brought against me.

NAME (PRINT)

ORGANIZATION

SIGNATURE

DATE SIGNED